National Aeronautics and
Space Administration
Headquarters
Washington, DC 20546-0001

Reply to Attn of: **Office of the Chief Information Officer**

MAR 2 7 2008

TO: Distribution

FROM: Chief Information Officer

SUBJECT: FY09 Acquisition of IT Products and Services Guidance

This guidance is being issued to assist Centers and Mission Directorates with the preparation of their fiscal year 2009 and out years budgeting for information technology (IT) resources, (e.g. products and services).

As you are aware, the Agency's Office of the Chief Information Officer (OCIO) has executed the IT governance process that will better align NASA's IT investments with the enterprise infrastructure initiatives. The six priorities of the infrastructure initiatives are:

- Define network perimeter and consolidate network management
- Establish Agency network visibility of IT assets and consolidate Agency security monitoring and management
- Enable cross-Center collaboration and strengthen user authorization
- Migrate systems to physically secure and properly managed data centers
- Make NASA's Information Easier to Discover and Access
- Standardize and consolidate the management of end-user devices

In the past, Centers and Mission Directorates have invested in IT resources to support and sustain their individual IT needs and requirements. With the execution of the enterprise infrastructure initiatives, acquisition of certain IT resources by Centers and Mission Directorates is no longer required.

To this end, Centers and Mission Directorates must immediately abstain from new investments for the following IT Security and Communication products and services:

1. Security Operations Center (SOC) – including the following technologies and services:
   - Security Event Managers (SEM) or Security Information Managers (SIM)
   - Network based Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS)
   - SOC managed flow monitoring tools (e.g. Qradar)
   - Incident Management databases

- Ticketing systems in support of SOC call centers
- SOC personnel to include:
  - SOC Incident managers,
  - Tier 1 personnel - SOC specific call center personnel
  - Tier 2 personnel - Incident detection and management (SIM/SEM monitoring)

2. Technologies such as Host based IDS/IPS and integrity checkers (e.g. Tripwire) will not be provided through the enterprise infrastructure initiatives at this time. However, Centers and Mission Directorates should prepare to transfer alerts generated from these products to the enterprise-wide SOC for tier 2 monitoring.

3. Data at Rest (DAR) encryption solutions for mobile media such as laptops and thumb/flash drives.

4. Networking hardware and software, – including the following technologies and services:
   - Network routers and switches to be used at what is currently the Center network border.
   - Firewalls for use at Center network border.
   - New purchase of network management software. Maintenance of existing systems should be maintained until such time as the Agency network operating center NOC has demonstrated management of Center assets.
   - Hardware and software related to web proxy services.

If you have any questions regarding acquisition of IT Security services and technology, please contact Jerry Davis, DCIO for IT Security at Jerry.I.Davis@nasa.gov. For acquisition questions in the area of communications, please contact Craig Hegemann, Deputy, Architecture and Infrastructure at Craig.Hegemann@nasa.gov.

Jonathan Q. Pettus